Clauses techniques

1. Objectifs

Le but de l'analyse consiste à évaluer et identifier les risques en matière de sécurité informatique de manière à ce que le pouvoir adjudicateur puisse prendre les mesures correctives nécessaire à la sécurisation de ses infrastructures et de ses logiciels.

2. Méthodologie

La méthodologie sera inspirée de l'Open Source Security Testing Methodology Manual (OSSTMM):

- Black Box : Sans connaissance des défenses, la cible n'est pas informée de la teneur des tests et audit. L'auditeur simule une attaque en se mettant dans la peau d'un hacker, dans les conditions d'un piratage réel. Cela signifie qu'il ne dispose d'aucune information sur sa cible ou de très peu d'éléments. Cette stratégie permet de définir avec fiabilité les seuils critiques de la sécurité d'une entreprise. Les pirates informatiques ne possèdent normalement que peu de données relatives au Système Informatique qu'ils tentent de compromettre. L'exploration du système d'information leur prend donc un certain temps, pendant lequel les entreprises ciblées peuvent réagir, si elles en ont les moyens. Le pentest BlackBox est donc approprié pour définir des scénarios en cas de tentative d'intrusion par une entité extérieure à l'entreprise.

- Grey Box : Les tests sont effectués en ayant une connaissance limitée des défenses et systèmes. Il s'agit d'une méthodologie intermédiaire, qui permet de bénéficier des avantages du BlackBox et du WhiteBox. Dans ce contexte, le pentester réalise son test d'intrusion en s'aidant d'un nombre restreint d'informations. Il peut, par exemple, intégrer l'entreprise en tant que salarié d'un service sensible et posséder son propre compte utilisateur. Au fur et à mesure qu'il progresse dans l'attaque, il obtient de nouvelles informations. Le GreyBox s'affirme comme une stratégie de pentesting optimale, puisqu'elle permet de simuler plusieurs types d'attaques, y compris celles réalisées « de l'intérieur ». Le pentester peut élaborer le scénario d'une attaque émanant d'un membre de l'entreprise ou d'un ancien salarié, voire d'un prestataire externe, en fonction des droits qui lui sont alloués.

- White Box : Similaire au Grey Box. La cible connaît cependant le périmètre et le planning des tests. L'auditeur travaille en étroite collaboration avec la Direction du Système Informatique de son client. Il accède à l'ensemble des informations relatives à la configuration du Système Informatique. Le pentest WhiteBox se rapproche davantage d'un audit informatique officiel, mais il offre la possibilité d'approfondir la détection des vulnérabilités en accédant à toutes les strates du système.

L'analyse comprendra les cinq étapes suivantes :

2.1 Reconnaissance

- Sert à définir la portée et les objectifs du test, y compris les systèmes et méthodes à utiliser.
- Une collecte d'information est effectuée pour comprendre le fonctionnement des serveurs, ordinateurs et imprimantes en visant des vulnérabilités potentielles. Il s'agit à la fois de scanner et connaître les systèmes (OS) utilisés et les ports ouverts, mais aussi l'environnement, pour en faire une topographie.

2.2 Énumération et Détection des vulnérabilités

- Interprétation des données collectées, analyse des services et ports (SMB, FTP, SSH, TELNET, SMTP, DNS, etc), adresses (type de réseau, Static/DHCP, vlan, routeurs, switchs, hubs) , exfiltration de données utilisateur (fichiers, mots de passe, etc…)

2.3 Exploitation

- Cette étape utilise des attaques systèmes, réseau et d'applications telles que les injections SQL, le Buffer Overflow, le Heap Overflow, le Brute forcing, etc afin d'exploiter les vulnérabilités présentes. Le but est de prendre le contrôle de machines et de faire « l'Escalades de privilèges », des mouvements latéraux afin de s'immiscer sur un maximum de machine, voire prendre le contrôle du « domain controler »

2.4 Post Exploitation

- Cette étape permet de voir si la vulnérabilité peut être persistante sur la machine exploitée afin de garder un contrôle permanent sur l'entreprise. Le but est de dérober des données sensibles le plus longtemps possible sans être détecté.

2.5 Reporting

Le rapport d'exécution :

- Background : description du but des tests et les définitions : vulnérabilité et contre-mesure.
- Posture globale : vue d'ensemble de l'efficacité des tests, les solutions trouvées (par exemple, l'exploitation de vulnérabilités connues) et les cas généraux permettant l'exploitation de vulnérabilités (cas du manque de mise à jour ou de patch).
- Profil du risque : classification générale de la posture sécuritaire de l'organisation.

Le rapport technique :

- Introduction : avec l'inventaire des détails tels que le périmètre du pentest, le(s) contact(s)…
- Récolte d'information : détails des informations récupérées durant la phase information-gathering.
- Évaluation de vulnérabilités : détails des découvertes durant la phase vulnerability-analysis du test.
- Vérification vulnérabilité/exploitation : détails des découvertes durant la phase d'exploitation du test.
- Post exploitation : détails des découvertes de la phase post-exploitation du test.
- Risques & dangers : une description détaillée des risques encourus.

3. Capacités techniques

A la demande du pouvoir adjudicateur le prestataire devra pouvoir fournir les éléments suivants :

- le personnel exécutant la mission devra avoir suivi une formation dans le domaine de la sécurité informatique et dispose des capacités techniques nécessaires.
- La preuve que l'entreprise existe depuis plus de 5 ans
- La preuve que le management de l'entreprise soumissionnaire pourra démontrer qu'il dispose de compétences scientifiques ou techniques avancées.

4. Périodicité et récurrence de l'analyse

Dans la mesure où de nouvelles failles de sécurité peuvent être découvertes quotidiennement, la présente analyse sera exécutée périodiquement pendant la durée du contrat.

La durée du contrat est fixée à (biffer les mentions inutiles) 1 an/ 2 ans / 3 ans / 5 ans
La fréquence d'analyse est (biffer les mentions inutiles) : Tous les mois/3 mois/6 mois/1 an

5. Livrable

Le livrable de la mission est un rapport dont le contenu est défini dans le paragraphe 2.5. Il sera mis à jour conformément à la fréquence d'analyse définie au point 4.

6. Prix

Le prix est constitué de deux postes inclus dans le tableau suivant qui sera complété par le soumissionnaire:

Poste	Description	Prix unitaire HTVA	Quantité	Sous-total HTVA
1	Analyse initiale	€	1	€
2	Analyses périodiques de mise à jour. Les quantités sont définies en fonction de la durée du contrat et de la fréquence de mise à jour.	€		€
	TOTAL HTVA			€
	TVA 21 %			€
	TOTAL TVAC			€

7. Facturation et paiements

La facture de l'analyse initiale peut être émise dès la signature du contrat.
Les factures des analyses périodiques seront établies à l'échéance de la période définie.

L'ensemble des factures sont payables à 20 jours calendrier.